

**Dan Roelker**  
**Program Manager, Information Innovation Office**

---

**Scaling Cyberwarfare**

DARPA Cyber Colloquium  
Arlington, VA

November 7, 2011



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>07 NOV 2011</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2011 to 00-00-2011</b>	
4. TITLE AND SUBTITLE <b>Scaling Cyberwarfare</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Defense Advanced Research Projects Agency (DARPA), Information Innovation Office, 3701 North Fairfax Drive, Arlington, VA, 22203-1714</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES <b>Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>7</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			



# Cyberartisan production doesn't scale

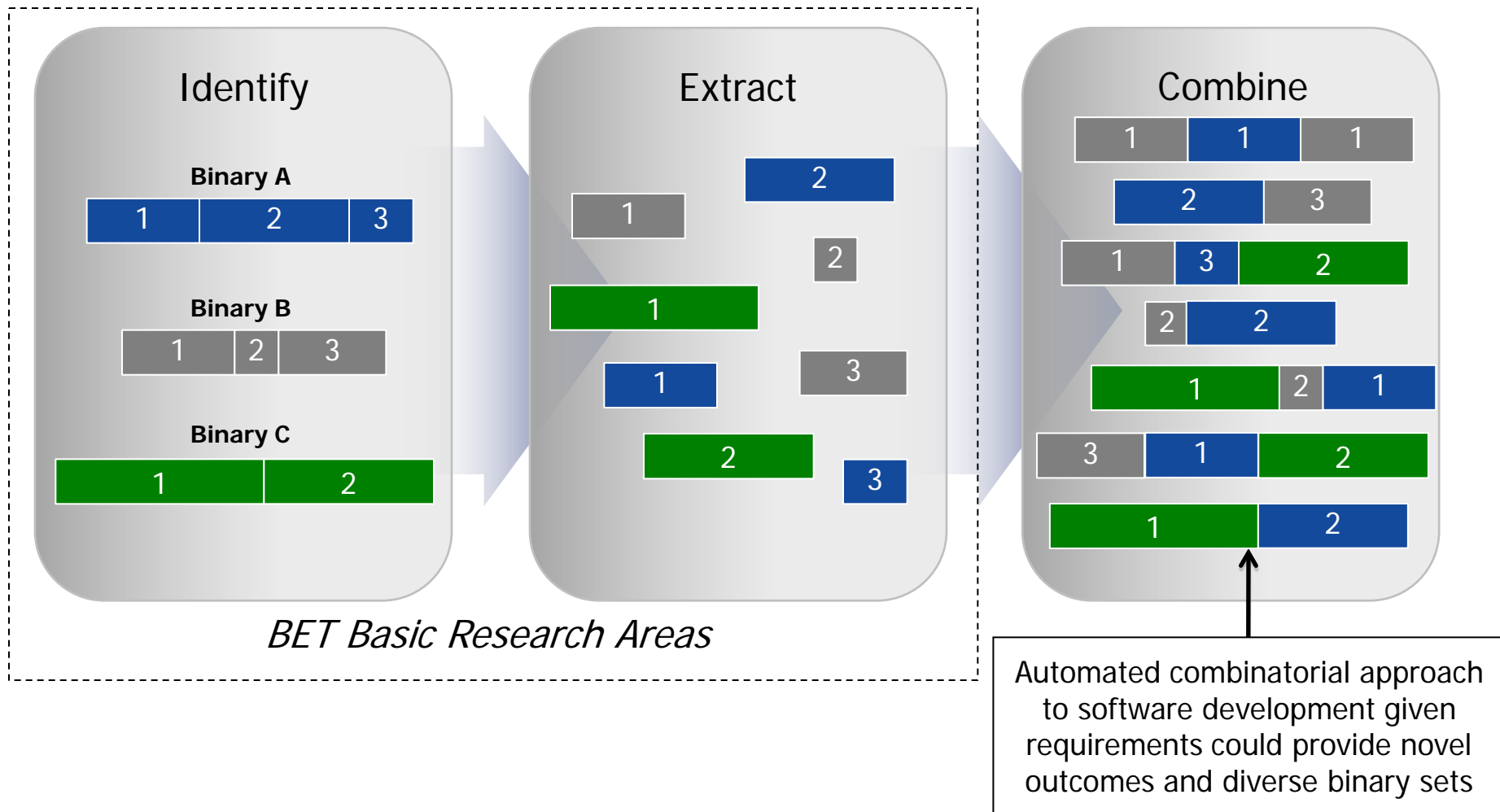


All cybertools have a limited shelf-life and operational relevance

	<i><b>Cyberartisan</b></i>	<i><b>Automation</b></i>
<b>Skill</b>	Individual	Technology-based
<b>Level of effort</b>	Manually intensive	Mass produced
<b>Cost/Benefit</b>	"Too big to fail"	Cost effective



# Program: Binary Executable Transforms (BET)



BET identifies and extracts functional components from binary executables with potential for reusing components in new combinations



# Hacker vs. Hacker approach doesn't scale



## Skill Level

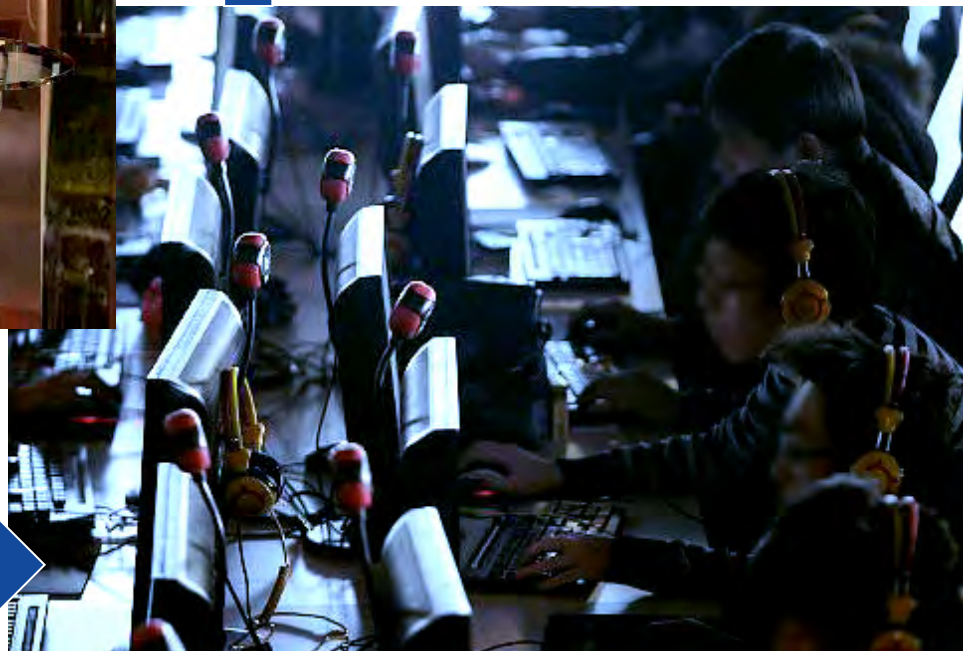
Not everyone can be the cyber equivalent of a Navy SEAL

## Scaling Limitations

Force size

Execution speed

Tactical depth



We don't win wars by out-hiring an adversary, we win through technology



# Limitations to the Hacker vs. Hacker approach

Cyberwarfare is executed at the speed of light . . .

## **Force Size Limitations**

#of people trained per year  
# of people to execute a mission

## **Execution Speed Limitations**

Speed of planning process  
Speed of mission operation

## **Tactical Depth Limitations**

Real-time move-counter-move  
Multi-phase mission strategy

we need breakthroughs in technology to accomplish this goal



# Pillars of Foundational Cyberwarfare

---

## Exploitation Research

automation techniques, defeating formal methods, high-fidelity emulation

## Network Analysis

on-demand topology, infrastructure capability, platform positioning

## Planning and Execution

assured and automated execution, large-scale analytics, distributed planning

## Cyberwarfare Platform Development

## Visualization

new interfaces, adaptable views, large-scale data representation



Ideas, thoughts, code? [daniel.roelker@darpa.mil](mailto:daniel.roelker@darpa.mil)

---